

ABSTRACT

5 The invention provides a form of reacting on security or vulnerability information relevant for a system comprising computer software and/or hardware or electronics, wherein a service provider with a first subsystem (1) is providing activation tokens to be received by a customer with a second subsystem (2). The activation tokens including activation information and naming of system characteristics in machine readable and filterable manner. The

10 second subsystem (2) comprises receiving means (11) for controlling the receiving of the activation tokens, checking means (12) for automatically determining whether the activation information is relevant for the second subsystem (2) by checking whether the second subsystem has characteristics corresponding to the naming of an activation token, and transforming means (13) for transforming relevant activation information into at least one activation measure for the second subsystem (2). The activation measures will reduce the vulnerability of the second subsystem.

15

DRAFT - 01/2020